Crypto-World

Informační sešit GCUCMP

ISSN 1801-2140

Ročník 10, číslo 2/2008 **17. únor 2008**

2/2008

Připravil: Mgr. Pavel Vondruška

Sešit je přednostně distribuován registrovaným čtenářům.
Starší sešity jsou dostupné na adrese
http://crypto-world.info
(1229 registrovaných odběratelů)

Obsah :

		str.
A.	O chystané demonstraci prolomení šifer A5/1 a A5/2	2-9
B.	Podmínky důvěryhodnosti elektronických dokumentů v archívu (Z.Loebl, B.Procházková, J.Šiška, P.Vondruška, I.Zderadička)	10-20
C.	Rozhovor na téma bezpečnost našich webmailů (.cCuMiNn. , P.Vondruška)	21-22
E.	O čem jsme psali v únoru 1999-2007	23-24
F.	Závěrečné informace	25

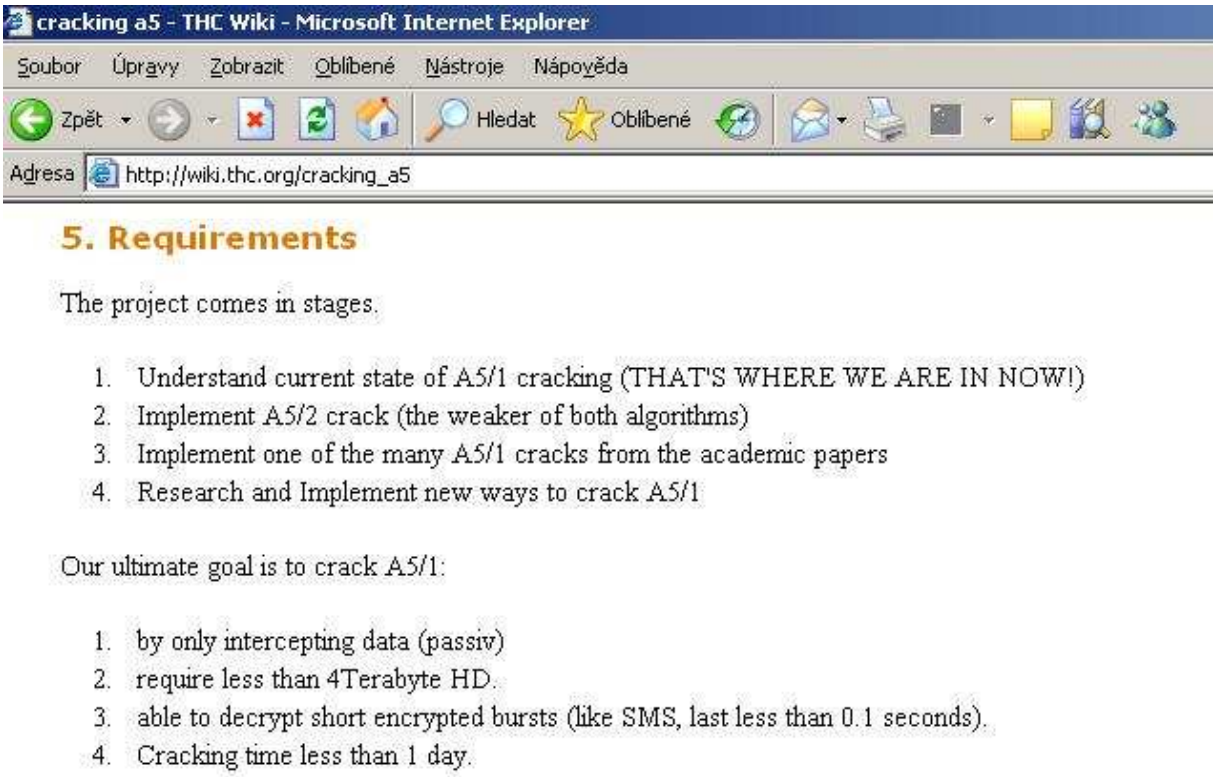
Příloha: ---

A. O chystané demonstraci prolomení šifer A5/1 a A5/2

Pavel Vondruška (pavel.vondruska@crypto-world.info)

Chystaná demonstrace útoku na A5/X (A5/1, A5/2)

Pravděpodobně již příští měsíc bude předvedena praktická ukázka prolomení šifer A5/1 a A5/2, která se používají pro šifrování dat při GSM komunikaci (přesněji mezi mobilním telefonem a nejbližší stanicí, kde se při autentizaci zaregistroval). Demonstraci této možnosti připravuje skupina, která je podporována organizací Electronic Frontier Foundation. Potřebné informace lze najít na stránce věnované přípravě tohoto projektu http://wiki.thc.org/cracking_a5.



Z cílů, které jsou jimi prezentovány plyne, že skupina chce v prvé fázi prokázat, že lze data při přenosu mezi mobilním telefonem a nejbližší BTS **zachytit a dešifrovat**. K tomu chtějí využít známé scénáře, které teoreticky rozpracovala akademická sféra v posledních devíti letech.

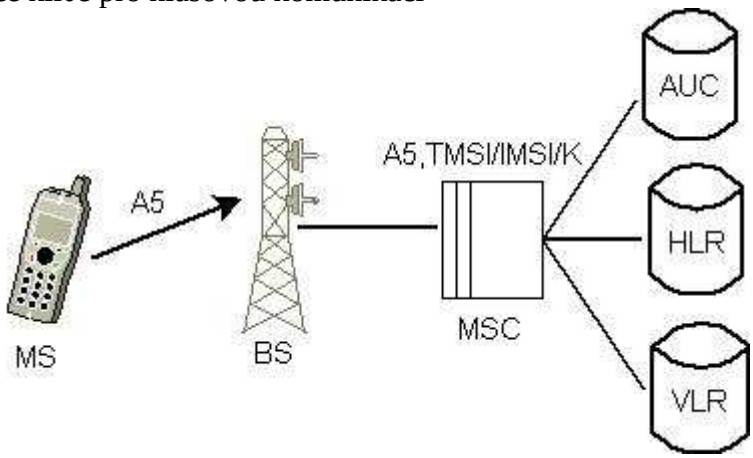
Dá se předpokládat, že ukázka praktického prolomení bude ve sdělovacích prostředcích bohatě komentována a jak už to při takových případech bývá, dá se očekávat, že možnosti útoku nebudou pochopeny a možnosti útočníka budou značně zveličeny. Speciálně se dá očekávat, že nebude dostatečně zdůrazněna technická složitost útoku (zejména odchytu dat), nutnost pohybovat se při odchytu dat v blízkosti uživatele a také se dá očekávat, že bude útok zaměněn za jiný útok, který má za cíl klonování karet a s tímto útokem nemá nic společného apod.

Jak to funguje …

Abychom lépe pochopili, co prolomení výše uvedených šifer A5/1 , A5/2 vlastně z hlediska bezpečnosti mobilních telefonů sítě GSM znamená, seznámíme se nejdříve s trochou teorie.

Zabezpečení stávajících mobilních telefonů GSM se opírá o autentizaci a zajištění důvěrnosti. Telefonní přístroj v souladu se standardem GSM budeme dále nazývat MT (Mobile Terminal), čipová karta, která se do něj vkládá, se nazývá SIM (Subscriber Identification Module). Po vložení SIM karty do MT máme k dispozici mobilní zařízení ("mobilní telefon"), které se nazývá MS (Mobile Station). Toto zařízení musí být zaevidováno u autentizačního centra (AUC) provozovatele. Norma předpokládá implementaci následujících šifrovacích algoritmů:

- A3 autentizační algoritmus
- A5/1 "silná verze" komunikačního algoritmu nebo A5/2 "slabá verze" komunikačního algoritmu (resp. A5/0 – tj. komunikační algoritmus, který neobsahuje šifrování)
- A8 generace klíče pro hlasovou komunikaci



Autentizace majitele GSM mobilní stanice (MS) a dohoda na klíči

K prověření identity SIM karty uživatele dochází vždy při vstupu do sítě a hlavní smysl tohoto mechanizmu spočívá v zabránění cizím osobám volat na náš účet.
Tajný klíč Ki, který je pro každého uživatele dané sítě jedinečný, je uložen v AUC a v modulu SIM. Na modulu SIM (čipové kartě) je Ki uložen tak, že jej není možné přečíst. SIM dovolí pouze s pomocí Ki provádět operace definované algoritmy A3 a A8.

Průběh autentizace je pak následující:
Uživatel stanice MS žádá o přihlášení do sítě po zapnutí MS. Po zadání pinu je spuštěn následující proces - síť od AUC zašle náhodné číslo RND do MS. Zde je číslo RND předáno modulu SIM, který na základě znalosti Ki a v SIM kartě uložených algoritmů A3 a A8 připraví trojici (RND, K3, K8). Hodnoty K3, resp. K8 spočte jako výstup z algoritmů A3 resp. A8 se vstupními parametry RND, Ki, tedy K3 = A3(RND, Ki) , K8 = A8(RND, Ki). Tato data jsou předána MS, který část K3 odešle do sítě a klíč K8 uloží zpět do SIM karty. Při požadavku na zahájení šifrovaného spojení je K8 použit jako klíč pro generování hesla algoritmem A5/1 resp. A5/2 .
Po obdržení K3 od MS provede síť test podmínky K3' = K3 (K3' si spočte AUC na základě znalosti Ki a jím odeslaného čísla RND). Pokud tato podmínka je splněna, prohlásí síť

provedenou autentizaci za úspěšnou a povolí přihlášení MS do sítě. V opačném případě je vstup do sítě odmítnut.
Algoritmy A3 a A8 v mnoha implementacích nahrazuje jediný algoritmus A38, který se také někdy označuje COMP128. Tento algoritmus (resp. jeho nepatrně pozměněné verze COMP128v2, v3) používá většina provozovatelů sítí GSM.

Malá odbočka - klonování karet

Tato malá odbočka vložena je úmyslně, protože se dá očekávat, že demonstrace útoku na algoritmuss A5/1 bude prezentována jako útok na zisk klíče, který umožní klonovat příslušnou SIM kartu a tedy v konečném důsledku útočníkovi telefonovat na účet vlastníka SIM karty. Ovšem není tomu tak, jak bude ukázáno dále, demonstrovaný útok na A5/X umožní pouze získat klíč, který je následně použit pro komunikaci (K8, nikoliv Ki). Pouze z jeho znalosti nelze provést naklonování příslušné SIM karty.

Prozatím není znám postup, jak zjistit Ki nějakého uživatele pasivním odposlechem komunikačního kanálu a odchycením dat během autentizace!

Metodu umožňující zjistit klíč Ki pro případ, že máme k dispozici přístup k SIM kartě zveřejnila v dubnu 1998 skupina kryptologů složená z pánů Marca Bricena, Iana Goldberga a Davida Wagnera. Karta se vloží do speciálního klonovacího zařízení spojeného s počítačem (na obrázku zařízení použité při pokusech o klonování karty v Berkley). Kartě jsou potom předkládány určité výzvy a analyzovány jsou reakce karty. Celkem je potřeba vznést cca 150 000 speciálně vybraných dotazů. Klonovací zařízení, které zkonstruovali, mohlo vyřídit 6.25 dotazů za vteřinu. K útoku s tímto zařízením bylo tedy potřeba asi 8 hodin. Pokud útočník vlastnící toto zařízení získal vaši SIM kartu na tuto dobu, byl schopen získat klíč Ki v ní uložený a vyrobit klon SIM karty. Je zřejmé, že se potom může do sítě autentizovat jako vaše SIM karta a účtovat hovorné na váš účet.
Útok byl dále vylepšován a podařilo se dobu potřebnou ke klonování snížit na 3-5 hodin.
Proti těmto útokům přijali operátoři v průběhu roku 2002 různá opatření. Například je na SIM kartě nastavený omezený počet přístupů (autorizací), tzn. že pokud dojde k překročení tohoto počtu, karta se stává nefunkční. A především přibližně od roku 2003 výrobci dodávají SIM karty, které jsou odolné proti výše popsanému a dalším modifikovaným útokům.

Útok byl postupně velmi popularizován. Program ke klonování byl zveřejněn a je na internetu volně dosažitelný. I v Čechách byla k této problematice zřízeno několik stránek. Na

jedné z nich je nabízen k prodeji i příslušný klonovaní hardware, zveřejněny jsou zde také návody a související poznatky http://klony.ic.cz/navod_na_vycteni_IMSI_Ki.htm

Důvěrnost přenášených dat

S pomocí zde popsané procedury se síť GSM snaží zabránit odposlechu hovorů přenášených vzduchem mezi mobilním telefonem a sítí GSM. K tomu slouží proudové šifrovací schéma A5, které využívá dočasný klíč (v našem značení K8), dohodnutý během poslední autentizační fáze.
(Poznámka. Kdyby zde tento algoritmus A5 nebyl implementován, byla by situace obdobná jako u bezdrátových telefonů, které lze celkem snadno odposlouchávat. Konverzaci lze odchytit vhodným skenerem až do vzdálenosti několika set metrů. Většina komerčních produktů totiž pro bezdrátový přenos hovoru mezi „ručkou“ a základnou nepoužívá šifrování http://www.upi.com/International_Security/Emerging_Threats/Analysis/2008/02/01/analysis_wireless_phone_headsets_insecure/2674/).

Data přenášená od MS směrem do sítě a data jdoucí opačným směrem procházejí různými kanály. Data jsou organizována po paketech, v kanálech se seskupují do úseků po 114 bitech a jsou vysílána po doplnění o synchronizační údaje v tzv. burstech.. Tato organizace je zavedena proto, že GSM používá metodu časového sdílení jednoho kanálu (TDMA – Time Division Multiple Access), která v jednom TDMA rámci vyhrazuje osm časových slotů. V každém z nich přitom může probíhat jiná komunikace.
Právě číslo rámce TDMA, v jehož časovém slotu je daný burst přenášen, se spolu s K8 podílí na generovaní hesla algoritmem A5. Číslo rámce je pro útočníka provádějícího pasivní odposlech známé.
Algoritmus A5 není z důvodu přenosové rychlosti implementován v SIM kartě, ale přímo v MT. Po algoritmu se požaduje, aby byl během trvání rámce (4,615 ms) schopen vygenerovat 228 produkčních bitů.

Proudová šifra A5/1

A5/1 je proudová šifra, která slouží k zabezpečení důvěrnosti a slouží pro zajištění bezpečnosti hovoru *ve vzduchu* při GSM komunikaci. Jedná se o typický proprietární algoritmus (její návrh byl držen v tajnost). Pomocí reverzní analýzy byl rekonstruován. Postupně bylo odhalena řada jeho slabin a byl teoreticky akademickou obcí prolomen.

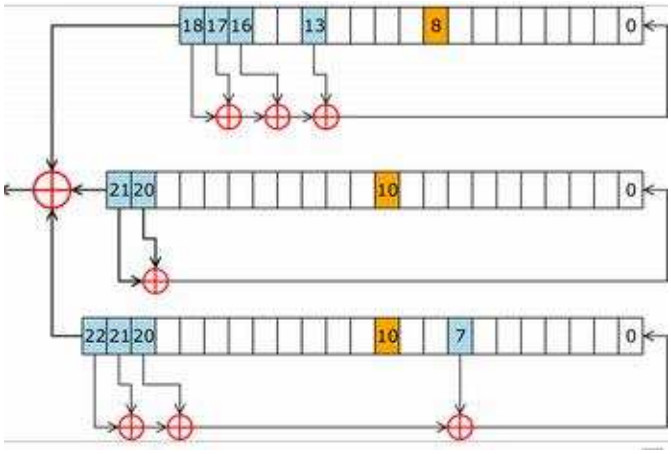
Historie a použití

Šifra A5/1 byla vyvinuta v roce 1987 v USA a v okamžiku kdy se GSM začalo používat ve východní Evropě a mimo Evropu (1989) byla vyvinuta odvezená mnohem slabší verze algoritmu, který je označován jako A5/2. Tato verze byla později v řadě států postupně nahrazována šifrou A5/1 (v současné době se používá algoritmus A5/2 již jen výjimečně např. v Srbsku nebo Keni). Při dalším rozšiřování GSM byla v některých regiónech dokonce zavedena komunikace, která není šifrována a dodnes se zde využívá (některé státy Afriky a Asie a to včetně celé Indie). Komunikační algoritmus bez šifrování nese kódové označení A5/0.

Algoritmy A5/1 a A5/2 byly utajovány. Prvé informace o obecné struktuře unikly v roce 1994. V témže roce Ross Anderson upozornil, že návrh může mít velmi vážné bezpečnostní slabiny. Marc Briceno v roce 1999 pomocí reverzního inženýringu detailně zrekonstruoval oba dva algoritmy.

Popis šifry A5/1

A5/1 je proudová šifra, která využívá zpětnou vazbu, konkrétně 3 registry (LFSR). Posuvný ("klokovací") bit má vliv na všechny 3 registry a je označen na obrázku oranžově.
Přenos dat GSM je organizován po sekvencích tzv. *bursts (shlucích).*
Typicky je pro přenos v jednom směru a jedním kanálem používána sekvenčně (shluk), který nese informaci 114 bitů a je odesílán každých 4.615 milisekund. Šifra musí zajistit ochranu pro komunikaci v obou směrech.
A5/1 je používána tak, že v tomto čase vyprodukuje bity, které jsou se shlukem téže délky sečteny pomocí XOR (pro dva kanály je tedy potřeba, aby proudová šifra vyprodukovala 2*114 bitů). A5/1 je inicializována klíčem délky 64-bitů a pomocí 22-bitového čísla rámce (TDMA). V GSM byla přibližně do roku 2001 použita implementace, kde prvních 10 bitů je dáno pevně a jsou nastaveny na 0. Výsledkem bylo, že klíč A8 má efektivní délku jen 54 bitů. V současné době má klíč A8 efektivní délku celých 64-bitů (algoritmy Comp128v2 a Comp128v3). Šifra A5/1 je tvořena třemi lineárními posuvnými registry R1, R2 a R3 o délkách 19, 22 a 23 bitů se zpětnou vazbou (LSFR), jak je uvedeno na následujícím obrázku.



Tyto tři registry lze algebraicky popsat takto:

Posuvný registr LFSR	Délka v bitech	Charakteristický polynom	Pulsní bit (clock)	Výstupní bity
R1	19	$x^{18} + x^{17} + x^{16} + x^{13} + 1$	C1 8	13, 16, 17, 18
R2	22	$x^{21} + x^{20} + 1$	C2 10	20, 21
R3	23	$x^{22} + x^{21} + x^{20} + x^{7} + 1$	C3 10	7, 20, 21, 22

Bity se číslují od nejméně významného bitu registru, tento bit je označen jako 0.
Pokud tedy označíme bit nejvíce vpravo indexem nula, má registr R1 zpětnovazební bity 18, 17, 16 a 13, pro R2 to jsou bity 21 a 20 a pro registr R3 bity 22, 21, 20 a 7. Prostřední bity registrů (u R1 je to bit 8, u R2 bit 10, u R3 bit 10) jsou určeny pro nelineární krokování a označíme je C1, C2 a C3. Jejich hodnoty určí, který z registrů bude stát a který se posune.

Krokování

Krokování je velmi jednoduché. Nejprve se vypočte majoritní (většinová) hodnota C a to takto: C se rovná nule, jsou-li alespoň dvě z hodnot C1, C2 a C3 nuly, jinak se rovná. Proto se

C rovná vždy buď dvěma, nebo třem bitům z trojice (C1, C2, C3). Krokování je definováno tak, že příslušný registr Ri se posune, pokud se hodnota jeho řídicího bitu Ci rovná majoritní hodnotě C (v každém kroku se proto posunou buď právě dva, nebo právě tři registry). Pokud posun nastane, je ze stávajícího stavu vypočtena zpětná vazba Z (například u R2 je to hodnota Z2 = $R_2$21 XOR $R_2$20) a ta se plní zprava do registru. Tím se zároveň posunou všechny buňky registru o jednu doleva.

Šifrování

Po ukončení tohoto posunu jsou vyčteny nejvyšší bity registrů a jejich XOR vytváří hodnotu hesla v daném kroku. Heslo se pak další operací XOR sloučí s otevřeným textem, který je takto postupně zašifrováván.

Počáteční naplnění registrů

K úplnému popisu ještě zbývá doplnit, jak se provede počáteční naplnění registrů. Nejprve se obsahy registrů vynulují a vypne se nelineární řízení. Všechny registry teď budou krokovat zcela pravidelně. Následně se připraví 88bitový proud, který je tvořen tajným klíčem Kc (64 bitů), následovaným 22-bitovým číslem rámce (TDMA). Jako první se z proudu použije nejnižší bit Kc a jako poslední nejvyšší bit TDMA. Následuje 88 kroků, v nichž se do zpětné vazby, jdoucí do nejnižšího bitu registru, „přixoruje“ navíc ještě také bit z našeho proudu. Proud je tímto způsobem plněn paralelně do všech registrů.
Protože registry mají jiné zpětné vazby i délky, jejich obsah bude nakonec jiný. Po dokončení tohoto kroku nazveme tento stav *počátečním stavem A5* (resp. jejích registrů). Protože byl vytvořen nezávislými lineárními kombinacemi bitů klíče (nelineární řízení bylo vypnuto), může se reálně dostat do všech 2^{64} možných stavů. Po úspěšném naplnění se nelineární řízení zapíná a pak následuje 328 kroků, v nichž je produkováno heslo. Jeho prvních 100 bitů se ignoruje, zbývajících 228 bitů h101 až h328 se použije pro zašifrování dat v obou kanálech tj. pro xor s daty o délce 2 x 114 bitů.

Bezpečnost

Postupně byly zveřejněny různé teoretické útoky na algoritmus A5/1. První úspěšné útoky byly založeny na složitých přípravných výpočtech (příprava rozsáhlé tabulky stavů), výsledkem však potom bylo umožnění luštění v řádu minut či dokonce vteřin. V roce 2003, byly odhaleny další slabiny, které umožňují zrychlit útok na šifrový text (se znalostí otevřeného textu). V roce 2006 Elad Barkan, Eli Biham a Nathan Keller demonstrovali útoky proti A5/1, A5/2, které umožňují útočníkovi prolomit GSM komunikaci v reálném čase nebo zachycenou komunikaci prolomit později.

Útok pomocí předvypočítaných stavů

Tento útok prezentoval Golič již v roku 1997. Složitost útoku (založeného na řešení velké matice lineárních rovnic) byla $2^{40.16}$. Tato složitost znamenala, že útok byl teoreticky možné provést.
V roce 2000 Alex Biryukov, Adi Shamir a David Wagner ukázali, že algoritmus A5/1 může být TEORETICKY prolomen dokonce v reálném čase užitím útoku zvaném time-memory

tradeoff attack. Důležitým momentem tohoto útoku je **přípravná fáze,** během které se vytvoří tabulka obsahující 2^{35} stavů automatu A5/1, která bude během lušticího procesu používána k určení vnitřních stavů. Autorům se podařilo vyvinout metodu, díky níž jsou schopni jednotlivé stavy kódovat pomocí 40bitových řetězců. Výsledná kapacita nutná pro uložení zmíněné tabulky tedy činí zhruba 146 GB (někdy se v literatuře uvádí více např. Wikipedia-EN uvádí hodnota 300 GB, ale tento údaj není vzhledem k možnostem současné VT podstatný, poznamenejme však, že disky této kapacity byly na hranici dostupnosti v době prezentace útoku). Přípravná fáze je náročná nejen na paměť, ale i na čas, neboť pro zkonstruování uvedené tabulky je třeba 2^{38} až 2^{48} operací. Vzhledem k těmto nárokům se přípravná fáze stává vzhledem k potřebným systémovým zdrojům nejnáročnějším krokem celé metody. Velmi závažné ovšem je, že výsledek této fáze je použitelný k útoku na A5/1 opakovaně kdekoliv a kdykoliv na světě (nezávisí na síti GSM operátora, jazyku apod.). Lze dokonce očekávat, že zmíněné tabulky naplněné potřebnými informacemi se mohou stát „obchodním artiklem"….
Koncem téhož roku Eli Biham společně s Orr Dunkelmanem publikoval vylepšený útok na A5/1 se složitostí $2^{39.91}$. Útok by teoreticky vyžadoval již jen 32 GB dat, které obsahují předvypočítaných 2^{38} stavů.
Následuje tabulka, která ukazuje na složitost některých typů útoků založených na předvypočítaných hodnotách a to z pohledu 4 nejdůležitějších parametrů : požadovaná velikost odchycených zašifrovaných dat, potřebná kapacita disku na uložení předvypočtených dat, počet „PC" potřebných k přípravě předvypočítaných dat – pokud bude požadováno, aby byla data shromážděna do 1 roku, doba výpočtu prolomení šifry A5/1 na 1 PC…

Table 1. Four Points on the Time/Memory/Data Tradeoff Curve for a Ciphertext-Only attack on A5/1

Attacked Channel	Available Data in Coded Messages (Four Frames)	Number of 250GBs Disks	Number of PCs to Complete Preprocessing in One Year	Duration of Online Phase on a Single PC in Minutes
KP* [7]	A Single Message	≈ 200	680	3.33
SACCH**	204 (≈ 3.5 min)	≈ 200	2800	13.33
SACCH**	600 (≈ 10 min)	≈ 200	930	1.53
SACCH**	600 (≈ 10 min)	≈ 67	930	13.83
SDCCH/8	204 (≈ 64 sec)	≈ 200	2800	13.33

* Known plaintext.
** The SACCH of the TCH/FS.

Další útoky na A5/1

Ekdahl a Johannson (2003) publikoval útok na inicializační stav algoritmu A5/1, který je možné provést po 2-5 minutách známé konverzace. Útok nepotřebuje přípravu a uložení předvypočítaných stavů.
V roce 2004 Maximov a kolektiv zdokonalil útok. Jejich metoda potřebuje již jen 1 minutu výpočtu a k realizaci stačí jen pár vteřin známé konverzace (znalosti otevřeného textu !).
Útok byl dále ještě vylepšen v roce 2005 a to pány Elad Barkanem a Eli Bihamem.
V roce 2003 Barkan a kol. publikovali několik možných útoků na GSM šifrování (mimo prosté zlomení šifry A5/1, A5/2 diskutují otázku men-in-the-midle). Zatímco dříve uvedené útoky nazývají pasivní tyto své nové řadí mezi aktivní. Základní myšlenkou je postavit mezi BTS a MT zařízení, které umožní vypnout A5/1 algoritmus v MS a místo něj zapnout A5/2. Následné „propustit autentizaci" MS na BTS a umožnit dokončit dohodu na klíči.

Připomeňme, že klíč je shodný pro A5/2 i A5/1. Komunikace útočníka je pak dvojí. S MS pomocí A5/2 a s BTS pomocí A5/1. Data (hovor) z MS dokáží teoreticky v reálném čase dešifrovat a zašifrovaný jej přenést dále na BTS. Útok zatím naráží na řadu technických problémů, ale jeho myšlenka je velmi zajímavá.
Dále ve své práci opět demonstrují, že šifra A5/2 je velmi slabá a šifra A5/1 je pomocí předvypočtených hodnot teoreticky prolomitelná.
V roce 2006 Elad Barkan, Eli Biham, Nathan Keller publikují PLNOU verzi svého předchozího příspěvku z roku 2003, která je věnována útokům na A5/X šifry.
Autoři tvrdí, že předkládají prakticky proveditelné útoky založené na kryptoanalýze zašifrované komunikace a dále některé možné útoky na GSM protokol (jako celek nejen na šifru A5/1).
Dá se předpokládat, že právě tato práce se stala základem pro projekt, který je uveden na začátku příspěvku.

Některé související odkazy

[1] Elad Barkan, Eli Biham and Nathan Keller, Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication, CRYPTO 2003, pp600–616 http://cryptome.org/gsm-crack-bbk.pdf
[2] Elad Barkan, Eli Biham and Nathan Keller, Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication, Technion - Computer Science Department - Technical Report CS-2006-07 – 2006 ,
[3] Eli Biham and Orr Dunkelman, Cryptanalysis of the A5/1 GSM Stream Cipher. INDOCRYPT 2000, pp43–51.
[4] Alex Biryukov, Adi Shamir and David Wagner, Real Time Cryptanalysis of A5/1 on a PC, Fast Software Encryption - FSE 2000, pp1–18 , http://cryptome.org/a51-bsw.htm
[5] Patrik Ekdahl and Thomas Johansson: Another attack on A5/1. IEEE Transactions on Information Theory 49(1), pp284–289, 2003 http://www.it.lth.se/patrik/papers/a5full.pdf .
[6] Jovan Dj. Golic, Cryptanalysis of Alleged A5 Stream Cipher, EUROCRYPT 1997, pp239–255 http://jya.com/a5-hack.htm .
[7] Greg Rose, A precis of the new attacks on GSM encryption, QUALCOMM Australia, 10 September 2003, http://www.qualcomm.com.au/PublicationsDocs/GSM_Attacks.pdf .
[8] Alexander Maximov, Thomas Johansson and Steve Babbage, An Improved Correlation Attack on A5/1, Selected Areas in Cryptography 2004, pp1–18.
[9] Elad Barkan, Eli Biham, Conditional Estimators: An Effective Attack on A5/1, Selected Areas in Cryptography 2005, pp1–19.
[10] A pedagogical implementation of the GSM A5/1 and A5/2 "voice privacy" encryption algorithms http://www.mirrors.wiretapped.net/security/cryptography/algorithms/gsm/a5-1-2.c
[11] Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication by Barkan and Biham of Technion (Full Version) http://www.cs.technion.ac.il/users/wwwb/cgi-bin/tr-get.cgi/2006/CS/CS-2006-07.pdf
[12] Technion team cracks GSM cellular phone encryption(Haaretz September 2003) http://www.cs.technion.ac.il/%7Ebarkan/GSM-Media/HaaretzInternetEnglish.pdf

B. Podmínky důvěryhodnosti elektronických dokumentů v archívu

Zbyněk Loebl, Barbora Procházková, Jaromír Šiška, Pavel Vondruška, Ivan Zderadička

1. Úvod

Problematika důvěryhodné archivace elektronických dokumentů patří k těm, jejichž vyřešení praxe potřebuje. Z hlediska dlouhodobého pohledu vyřešení této otázky je zcela nezbytné. Množství informací, se kterými lidstvo pracuje, narůstá zvyšujícím se tempem. Pokud nenalezneme vhodné cesty k úschově těchto informací (a to dlouhodobé úschově), hrozí nebezpečí, že některé nám již známé informace se k budoucím generacím ani nedostanou.
Autoři tohoto příspěvku tvoří tým, který vypracoval výzkumný projekt „Dlouhodobé uchovávání elektronických dokumentů se zaručeným elektronickým podpisem“, financovaný Ministerstvem informatiky a následně Ministerstvem vnitra ČR v roce 2007 (dále jen Projekt). Tento příspěvek vychází z Projektu. Vzhledem k tomu, že v rámci tohoto příspěvku není možné zabývat se všemi otázkami, souvisejícími s výše uvedeným nadpisem našeho příspěvku, odkazují autoři zájemce o detailnější studium problematiky na webové stránky http://digiarchiv.eu/ .

Z provedené analýzy problému, standardů a projektů vyplynulo, že stanovit konkrétní požadavky na „obecný“ archiv elektronických dokumentů, po kterém se „volá“ v abstraktu, je velmi komplikované a to zejména z důvodu, že ukládání dokumentů nějakým subjektem do archívu sebou nese různá (často odlišná) očekávání na to co má archív ED vlastně zajistit. Tyto požadavky nejčastěji vycházejí z legislativy, ale mohou být také svázány s komerčními požadavky (a to jak provozovatele archívu tak subjektu, který ED do něj vkládá) nebo mohou být výsledkem subjektivního chápání jedince, který chce služby archívu využít pro svoji potřebu.
Mezi typické speciální požadavky vycházející z legislativy lze řadit požadavky na ukládání elektronických daňových dokladů (konkrétní minimální doba úschovy, zachování integrity a původu po celou dobu úschovy, dostupnost a převod do čitelné formy - Směrnice Rady 2001/115/ES). Jinými důvody ukládání ED, které mohou nabýt masových rozměrů, může být naopak úschova „elektronických archiválií“ po velmi dlouhou dobu.

Pojem „původ dokumentu“ se však v obou uvedených případech velmi zřetelně liší. V prvém případě je potřeba prokázat, kdo je skutečným vystavitelem příslušného daňového dokladu a zachovat „nepopiratelnost“ v tohoto vyhotovení (autenticita původce), ve druhém případě je původ vnímán jako úschova důvěryhodné informace o tom, jak byl dokument získán a předpokládá se, že otázka spojená s tím, kdo a kdy dokument vytvořil, se řešila před přijetím resp. při přijetí dokumentu do archívu. V prvém případě je otázka průkaznosti původu kritická pro to, aby mohl být takový doklad použit jako „pravý“ daňový doklad („nepopiratelnost“), ale ve druhém případě není podstatná „pravost“ dokumentu, neboť jako archiválie může mít význam i falzifikát, který dokonce právě z tohoto důvodu může mít svoji historickou hodnotu a může být archivován. U uchovávání archiválií v elektronické podobě je tedy důležité akcentovat obecně jiné požadavky než u daňových dokladů. V případě obecných archiválií je nutné zejména zajistit po celou dobu úschovy integritu, čitelnost (tj. uložení ve vhodném formátu nebo zajistit transformaci do jiného formátu bez „ztráty obsahové nebo jiné informace, která má být archivována“) a důvěryhodným způsobem archivovat doplňující informace, které (mimo jiné) popisují původ dokumentu.

Při návrhu konkrétního elektronického archívu je proto potřeba rozhodnout, zda bude také sloužit i pro vkládání ED, kde má být uchován zaručený elektronický podpis. Zda tedy půjde o úschovu ED, které mají být později použity zejména z hlediska nepopiratelnosti a kde je pro tento důkaz zaručený elektronický podpis nezbytný (nebo je vyžadován příslušnou legislativou). V návrhu takovéhoto elektronického archívu se nelze vyhnout zásadnímu problému při archivaci, kdy autentizace dokumentu je vázána na podpisová schémata použitá pro vytvoření zaručeného elektronického podpisu. V takovém případě je integrita dokumentu zajišťována až na úrovni hodnot jednotlivých bitů přijatého dokumentu. Pokud je potřeba provést transformaci dokumentu (například převod z jednoho formátu na jiný) nelze toto provést bez narušení takto fixované integrity dokumentu. Dalším významným problémem je „stárnutí“ použitých algoritmů pro použité podpisové schéma. Může se stát, že po několika letech se najdou metody nebo bude dostatečná výpočetní kapacita, aby bylo možné z veřejného klíče odvodit soukromý klíč a tím narušit vyžadovaný princip nepopiratelnosti. Otázky spojené s úschovou takovýchto dokumentů vyžadují velmi specifický přístup a není zde ještě dokončen vývoj norem, případně obecná shoda na správném přístupu (viz přístupy jako Trusted Archival Services, projekt ltans, protokoly DVCS, TAP, TAA, ..).

Jinou velmi specifickou oblastí může být ukládání obsahu sledovaných internetových zdrojů (portály, e-ziny, weby institucí). Zde je problém spojen především s otázkou „dynamiky“ stránky a z hlediska dlouhodobé archivace s otázkou vývoje použitých formátů.

Z výše uvedeného plyne, že archiv elektronických dokumentů nemůže, alespoň v této fázi „poznání” zajistit „všechno” a bude pravděpodobně nutná určitá specializace v nabízených službách dlouhodobé elektronické archivace.

Náš koncept, který je popsán v Projektu, je jakýmsi propojením požadavků vycházejících z LRG definic (Research Libraries Group, 2002) [1] a podmínek uvedených v organizačním konceptu a katalogu projektu DOMEA-Konzept (Requirement Catalogue 2.0 , 2005) [2].

Velmi stručně lze charakterizovat předpokládané řešení jako orientaci na zajištění těchto požadavků:

- shoda se standardy (zejména OAIS, Ltans, …)
- administrativní záruky za uložená data
- schopnost vývoje a reakce na změny
- finanční udržitelnost po celou plánovanou dobu projektu
- technologická a procedurální přiměřenost
- odpovídající systémová bezpečnost
- procedurální zodpovědnost.

2. Legislativní předpoklady elektronické archivace

V rámci studie se velmi detailně zabýváme právními a souvisejícími obchodními a organizačními aspekty dlouhodobé bezpečné archivace dokumentů v elektronické formě (dále jen „elektronická archivace“).
Základní úprava právních otázek, spojených s elektronickou transformací a archivací, byla upravena již v roce 1996 v UNCITRAL Model Law on Electronic Commerce [3], (dále jen „UNCITRAL Model Law“). Tento modelový zákon je od doby svého vzniku inspirací pro nejrozvinutější státy světa při přípravě své národní legislativy (např. USA a Francie – viz níže) a vychází z něj např. i Evropská komise při přípravě evropské legislativy, řešící některé aspekty elektronické komunikace [4].

UNCITRAL Model Law

UNCITRAL Model Law vychází ve své úpravě z důsledného technologicky neutrálního přístupu a z rozlišení pojmu „písemnost“, „originál“, „podpis“, „úřední/notářské ověření“, „právní účinek/důkazní síla“ a „archivace dokumentů“. V podstatě lze uvést, že UNCITRAL Model Law definuje „písemnost“ na nejnižší úrovni požadavků jako cokoliv v jakékoliv formě a na jakémkoliv nosiči, co je možno reprodukovat a číst pro účely budoucího využití (viz Čl. 6). Za písemnost by tedy měly být považovány např. veškeré e-mailové zprávy nebo libovolné texty v elektronické formě, bez ohledu na úroveň jejich zabezpečení nebo na to, zda je z nich patrný jejich zdroj.
Dále, UNCITRAL Model Law definuje pojem „originál“, a to nikoliv ve vztahu k formě, v jaké byl příslušný dokument původně pořízen, ale ve vztahu k integritě obsahu příslušného dokumentu (viz Čl. 8). Za originál by tedy bylo možno považovat i n-tou elektronickou kopii dokumentu, pokud by bylo možné prokázat integritu jeho obsahu od okamžiku, kdy byl vyhotoven ve své finální formě. Jak uvidíme dále, toto pojetí bylo převzato v USA.
Ve Francii a Velké Británii je toto ustanovení UNCITRAL Model Law komentováno v tom smyslu, že je obtížné mluvit v moderní době o originálu dokumentu v elektronické formě a že je lépe pojem originálu vůbec opustit. Naopak, je třeba se zaměřit na stanovení obecných podmínek, za nichž mají dokumenty v libovolné formě (papírové či elektronické či jiné) plný právní účinek/důkazní sílu, srovnatelnou i s originály papírových dokumentů.
UNCITRAL Model Law uvádí obecné podmínky, ovlivňující plný právní účinek/právní sílu elektronických dokumentů v Čl. 9 odst. (2). Toto ustanovení klade důraz na zajištění integrity informací, autentičnost původce a na důvěryhodnost procesu vytváření, ukládání a komunikace datových zpráv. Splnění těchto podmínek je do značné míry ovlivněno požadavky na důvěryhodný (zaručený) elektronický podpis. UNCITRAL Model Law obsahuje požadavky na elektronický podpis v Čl. 7.
Konečně, UNCITRAL Model Law upravuje rovněž výslovně elektronickou transformaci a archivaci dokumentů (viz Čl. 10). Úprava vychází z pojetí originálu, písemnosti a plné právní účinnosti/důkazní síly, a v podstatě spojuje všechny požadavky, zmiňované výše. V odst. (1) tohoto ustanovení se uvádí následující tři požadavky (skupiny požadavků) na datovou zprávu, která by měla splňovat požadavky na dlouhodobou archivaci dokumentů v libovolné formě:

- požadavky na písemnost (reprodukovatelnost a čitelnost);
- datová zpráva by měla být archivována ve formátu, v němž byla vytvořena, odeslána nebo přijata (tedy originální formát), nebo ve formátu, který umožňuje přesné zachování vytvořené, odeslané nebo přijaté informace (toto ustanovení směřuje k transformaci papírových dokumentů do elektronické formy); a
- taková informace by měla umožňovat určení původu a místa určení příslušného dokumentu a času, kdy byl dokument odeslán nebo přijat.

Evropská unie

V rámci legislativy EU jsou důležité zejména Směrnice EU č. 1999/93/ES o elektronických podpisech, Směrnice č. o 2000/31/ES elektronickém obchodě a Směrnice č. 2001/115/ES o DPH.
Dále, v rámci EU se zpracovává celá řada standardů a doporučení, která jsou velice důležitá pro oblast elektronického archívnictví (viz Projekt, příloha 6.1).

Vybrané jednotlivé státy

USA

Obecná zákonná úprava

Elektronická komunikace

V USA v roce 1999 vypracovali americkou obdobu UNCITRAL Model Law, tzv. Uniform Electronic Transactions Act (1999). Tento návrh zákona vypracovala National Conference of Commissioners of Uniform State Laws, která připravuje unifikované zákony pro jednotlivé státy USA. V mezidobí tento zákon přijala naprostá většina států USA. Dále, v roce 2000 byl přijat federální zákon o elektronickém podpisu, tzv. E-Sign Act. Oba právní dokumenty vycházejí v podstatné míře z UNCITRAL Model Law, tento právní model však dále rozvíjejí. Oba legislativní texty představují v současné době pravděpodobně nejmodernější komplexní právní úpravu elektronických obchodních transakcí, uznávanou mezi odborníky na celém světě.

Speciální zákonná úprava

Elektronická archivace a transformace

Uniform Electronic Transactions Act (UETA) upravuje problematiku elektronické transformace a archivace v Čl. 12. UETA zahrnuje pod požadavky na pojem originálu (odst. (d)) požadavky na elektronickou transformaci a archivaci (odst. (a)) a požadavky na plný právní účinek/důkazní sílu elektronických dokumentů (odst. f)). Obdobná úprava je obsažená ve federálním E-Sign Act, čl.1 odst. (d).
Vzhledem k tomu, že z působnosti UETA a E-Sign Act jsou vyňaty některé typy dokumentů, byl pro tyto dokumenty připraven v roce 2004 Uniform Real Property Electronic Recordation Act (URPERA). Název napovídá, že se jedná zejména o dokumenty, vztahující se k vlastnictví nemovitostí. Tento modelový zákon není platným zákonem, byl vypracován zmiňovanou National Conference of Commissioners of Uniform State Laws a je určen pro implementaci jednotlivými státy USA.
URPERA obsahuje nejen úpravu elektronické archivace, ale i transformace v Čl. 3, 4 a 5. URPERA výslovně umožňuje elektronickou transformaci a archivaci (Čl. 4), včetně nahrazení požadavku na předložení originálu dokumentu jeho elektronickým záznamem (Čl. 3). Nicméně, nestanoví obecné požadavky jako UETA a E-Sign Act, ale odkazuje na zvláštní komise vytvořené na státní úrovni (tzv. state electronic recording commissions – Čl. 5), které by měly formulovat standardy pro elektronickou správu dokumentů, které spadají pod URPERA.

E-discovery (povinná archivace)

Další úpravou v USA, která reflektuje novodobý vývoj je od 1. prosince 2006 účinná změna občanského soudního řádu. Dodatek schválený Nejvyšším soudem v dubnu 2006 reflektuje nutné změny v procesním právu (tzv. e-discovery rules), neboť tradiční procesní pravidla vztahující na důkazy v papírové formě nelze použít pro úpravu problematiky elektronických dokumentů, např. automatický vznik metadat, znovuzískání vymazaných dat či všeobecně obrovské množství informací v elektronické podobě.

Novela občanského soudního řádu specificky zahrnuje elektronické informace mezi důkazní prostředky. Avšak vzhledem k tomu, že množství elektronických informací může být v rámci společností obrovské a zahrnuje například i informace z archivu, záložních pásek, testovacích systémů či údaje ze starších „počítačů“ (legacy data), což může vést mimo jiné k neúměrným výdajům v souvislosti s obstaráváním takovýchto důkazů, stanovuje další pravidla.
Mezi tyto pravidla patří možnost specifikace formátu, ve kterém elektronické informace mají být předloženy a možné námitky vůči předloženému formátu, dostatečná specifikace záznamů umožňující snadnou identifikaci potřebných informací, vyloučení důvěrných informací či těch informací, které nejsou přijatelně přístupné z důvodů obtížnosti nebo nákladů.
Výsledkem je, že americké společnosti by měly mít přehled o všech elektronických informacích a stanovit „přiměřenou“ archivní politiku vůči všem schraňovaným elektronickým informacím (nejenom dokumentům a e-mailům) a věnovat jí náležitou pozornost v případě hrozících soudních sporů či již probíhajících soudních sporů či vyšetřování. V takovýchto případech by společnosti měly zajistit uchování relevantních dat včetně ohledu na jejich formát, jinak jim hrozí nepříjemně vysoké pokuty, včetně trestu odnětí svobody. Výjimku představují případy, kdy ke ztrátě informací dojde v důsledku rutinní operace elektronického informačního systému v dobré víře.

Velká Británie

Judikatura

Velká Británie dosáhla obdobného právního stavu jako USA, nikoliv však na základě zvláštních zákonů, ale zejména na základě soudních rozhodnutí. Jak již bylo uvedeno výše, anglické právo prakticky zrušilo požadavek na originál dokumentů. Ve Velké Británii byly rovněž vydány první soudní rozhodnutí, které přiznaly plný právní účinek a důkazní sílu elektronickým dokumentům [7]. Tato rozhodnutí sledovala obdobné požadavky, jako jsou obsaženy v UNCITRAL Model Law. Navíc, Velká Británie jako člen EU přijala zákony, implementující Směrnice EU významné pro sledovaný problém, zejména Směrnici č.1999/93/EC o elektronických podpisech, Směrnici č. 2000/31/EC o elektronickém obchodu a Směrnici č. 2001/115/EC, upravující fakturaci pro účely DPH včetně elektronické fakturace.

Obecná zákonná úprava

Zákon o elektronických komunikacích stanovuje, že elektronický podpis je důkazním prostředkem v soudním řízení a slouží k autentizaci (ustanovení 7). Je však vždy na soudci, aby uvážil, zda byl elektronický podpis řádně použit. Ustanovení 7 zákona o elektronických komunikacích ale nestanovuje podrobnosti týkající se elektronického podpisu, jako jeho formát či užité metody. Legislativa se snaží být technologicky neutrální a vztahuje se na různé typy elektronických podpisů počínaje těch užívaných v e-mailové korespondenci přes elektronické podpisy s využitím kryptografie až po biometrická data. Všeobecně lze říci, že znakem britské legislativy je do určité míry liberální přístup.

Francie

Obecná zákonná úprava

Elektronická komunikace

Francouzské právo bylo významně upraveno ve vztahu ke sledované problematice v roce 2000. Francouzský občanský zákoník opět vychází z UNCITRAL Model Law a definuje obdobně písemnost (Čl. 1316).
Dále se občanský zákoník zaměřuje na stanovení obecných požadavků na plný právní účinek/důkazní sílu elektronických dokumentů (Čl. 1316-1). Uvedené požadavky opět odpovídají požadavkům uváděným v UNCITRAL Model Law, ve zmiňovaných právních

předpisech v USA nebo soudních rozhodnutí ve Velké Británii, tedy autentičnost původce a integrita obsahu.
Navíc občanský zákoník stanoví v Čl. 1316-3, že požadavky na právní účinek/důkazní sílu jsou shodné u papírových a elektronických dokumentů. Zákon přiznává dokumentu, který byl původně vytvořen v elektronické podobě hodnotu originálu, ale je třeba jej vybavit možností ověření a integrity obsahu – proto tyto dokumenty jsou opatřeny elektronickým podpisem.

Specielní zákonná úprava
Elektronická fakturace
Oblast elektronické fakturace je upravena nařízením ze dne 18. července 2003 a daňovým předpisem z 7. srpna 2003. Elektronická faktura může být předána ve dvou formátech: ve strukturovaném (EDI) a v nestrukturovaném, kdy dokument musí být opatřen elektronickým podpisem.,.
Faktura je přijata daňovým úřadem, jestliže splňuje určitá kritéria: musí obsahovat všechny obligatorní zákonné náležitosti , být v souladu s direktivami o DPH, odpovídat pravidlům uchovávání dokumentů, odpovídat účetním závazkům podniků a obchodu.

Podnik může externalizovat dematerializaci svých faktur prostřednictvím platformy nebo operátora elektronické fakturace. Dodavatel podepisuje smlouvu o službách (certifikačních, mandátních), která vyžaduje souhlas (alespoň tacitní) klienta.
Pro EDI, XML francouzská úprava (v rozporu s evropskou směrnicí) požaduje s transakcí EDI zaslat i papírový originál nebo dodržovat tři přísná kritéria dovolující vyhnout se dvojímu papírování, a to:
odesílatel i zákazník musejí uchovávat elektronický originál v elektronickém trezoru
je nutné každodenně vést seznam všech vyměněných faktur včetně chyb i anomálií
je nutné vést si seznam partnerů, se kterými dochází k výměně faktur.

Code Général des Impôts, článek 289, definuje dematerializaci faktur, vystavovatel faktury musí zabezpečit totožnost vydaných a doručených zpráv, zatímco příjemce nakládá s fakturou tak, jak ji obdržel. Každá ze stran přitom může používat svůj vlastní nástroj k dematerializaci faktur při dodržování určitých standardů. Dokumenty je nutné podepsat elektronickým podpisem. Výměna dematerializovaných faktur mezi stranami nemusí být ověřena třetí osobou, toto nelze právně vynutit.

3. Přehled relevantních standardů

Existuje mnoho kategorií standardů, zabývajících se tvorbou bezpečných informačních systémů a standardizací souvisejících problémů. Výběr a volba konkrétních standardů má pak přímý nebo nepřímý vliv na výsledné řešení tj. v našem případě na archív elektronických dokumentů. Jde zejména o standardy mezinárodní, regionální (např. evropské standardy), národní standardy, standardy státní správy některého státu, standardy určitého zájmového sdružení nebo průmyslové standardy. V tomto konkrétním případě pak je problematika natolik nová, že otázky spojené s konkrétními bezpečnostními protokoly doporučenými pro použití v elektronickém archívu často ještě nejsou součástí oficiálních standardů (např. standardizační „cesta“ ISO norem trvá několik let) a je nutné se při výběru soustředit na standardy de-facto resp. standardy připravované různými zájmovými skupinami nebo doporučené postupy, které byly vytvořeny v rámci projektů.

Správná volba standardu může být proto velmi komplikovanou záležitostí. Obecně platí, že význam každého z těchto standardů zcela závisí na rozsahu jeho použití. Tento rozsah použití

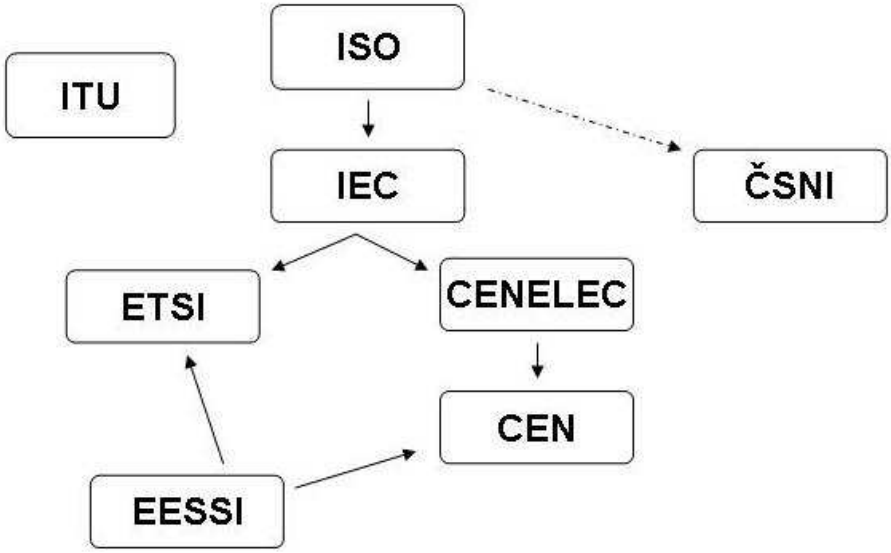
nemusí vždy odpovídat úmyslům tvůrců standardu (například standardy PKCS). Známe mnoho případů, kdy ambiciózní standardy (vyvinuté např. v průběhu na podporu konkrétního projektu) upadly nakonec v zapomnění, nebo kdy původně zcela opomíjený standard získal posléze celosvětový význam (třeba RFC standardy).

Volba vhodného standardu v případě archívu, který má působit řadu let, je tak velmi složitou právě z hlediska toho, že nově vytvářené de-facto standardy nebyly ještě prověřeny v masovém nasazení a případně v „konkurenčním boji" s řešeními, která se nabízejí jako výsledky jiných projektů. Problém je také s tím, že tato doporučení nemusí být ještě kodifikována a mohou zaniknout nebo být nahrazeny jinými. Zpravidla platí, že nejširší platnost a z hlediska času nejdlouhodobější mají standardy mezinárodní a regionální a tedy pokud takovýto standard existuje mělo by se k němu přednostně přihlédnout. Dále je potřeba při výběru těchto standardů de jure vzít do úvahy, že použití národních standardů a standardů státní správy zpravidla nepřesahuje hranice státu, ve kterém byly tyto standardy vytvořeny. Výjimkou z tohoto pravidla jsou národní standardy USA (označované ANSI) a standardy státní správy USA (FIPS), které jsou někdy používány i mimo hranice USA a které proto mohou být vnímány jako vhodná doporučení při tvorbě elektronického archívu.

V neposlední řadě je potřeba také vzít při výběru do úvahy právní závaznost některých standardů. Takovouto právní závaznost mívají až návrhy ve formě **norem**, které v rámci jednotlivých zemí vypracovávají k tomu oprávněné instituce, často na základě doporučení přijatých mezinárodními organizacemi. Právní závaznost tyto normy mít však nemusí – záleží na postavení národní normotvorné instituce a konkrétní národní legislativy.
V ČR bývají technické normy pouze kvalifikovanými doporučeními a nejsou závazné. Jejich používání je dobrovolné, avšak všestranně výhodné. Jejich použití je ale na druhé straně často nezbytnou podmínkou pro volný oběh zboží a služeb zejména v EU. Slouží především jako referenční úroveň, k níž se poměřuje úroveň výrobku nebo služby a stanovují kritéria bezpečnosti. Bývají také efektivním nástrojem konkurenčního boje. V obchodních smlouvách mezi dodavatelem a odběratelem se obvykle stávají závaznými a bývají také povinně vyžadovány u veřejných zakázek.

Členění relevantních standardů dle vystavitele

ISO - International Organization for Standardization (Mezinárodní organizace pro normy)
ČSNI - Český normalizační institut
IEC- International Electrotechnical Commission (Mezinárodní elektrotechnická komise)
ETSI – European Telecommunication Standards Institute (Evropský ústav pro telekomunikační normy)
CEN – European Commitee for Standardization (Evropská komise pro normalizaci)
CENELEC - European Committee for Electrotechnical Standardization (Evropská komise pro elektrotechnickou normalizaci)
EESSI - European Electronic Signature Standardisation Initiative (Evropská iniciativa pro standardizaci elektronického podpisu)
ITU – International Telecommunication Union (Mezinárodní telekomunikační unie)
ANSI – American National Standards Institute (Americká národní standardizační organizace)
FIPS – Federal Information Processing Standard
RFC – Request for Comments



Vztahy přejímání standardů a oblastí, které jednotlivé organizace upravují.

Členění relevantních standardů podle oblasti, kterou upravují:

- **základní standardy** - pro obecné požadavky
- **kritéria hodnocení dosažené bezpečnosti** - pro hodnocení produktů a systémů
- **standardy upravující kryptografické algoritmy** – asymetrická kryptografie, hašovací funkce, náhodné generátory, protokoly, ..
- **standardy upravující oblast PKI** – certifikáty, poskytovatelé certifikačních služeb, atributy
- **standardy upravující zaručený elektronický podpis** - typy elektronických podpisů, časové značky
- **protokoly upravující důvěryhodnost archívu** – TAA, TAP, DVCS
- **standardy pro bezpečnostní procesy** – systémy řízení bezpečnosti
- **speciální standardy zabývající se úschovou elektronických dokumentů –** např. ISO 15489 Standard for Record Management
- **standardy definující formáty elektronických dokumentů –** XML, PDF, **...**
- **výkladové dokumenty** -- průvodce, slovníky pro informovanost a vzdělání

Subjektivní členění relevantních standardů podle významu:

- **„Běžné standardy“ –** standardy běžně používané při vývoji projektu, který se zabývá výstavbou rozsáhlého IT systému a to včetně řízení bezpečnosti a hodnocení dosaženého stupně bezpečnosti
- **„Standardy pro bezpečný archív**“ – specifické standardy, které byly vyvinuty nebo použity při návrhu obdobného řešení, zejména standardy, které upravují bezpečnostní protokoly pro dlouhodobou důvěryhodnou archivaci
- **„Legislativní standardy“** – výběr standardu není možný, ale je dán tím, že má být zajištěn některý požadavek národní legislativy

Podrobný přehled relevantních standardů je uveden v závěrečné zprávě projektu[Projekt].

4. Přehled relevantních projektů

Využití dokumentů v elektronické podobě je stále širší díky rozvoji informačních technologií a také díky posunu v legislativní podpoře elektronických dokumentů (jako je např. EU direktiva o digitálním podpisu). Stále narůstající počet dokumentů vytvářených a zpracovávaných v elektronické formě také vytváří potřebu pro jejich dlouhodobé uložení. Tato potřeba byla rozpoznána řadou národních a mezinárodních organizací a do současné doby byla započata nebo již realizována široká škála projektů v této oblasti.

První projekty, které se touto problematikou začaly systematicky zabývat, začínaly v devadesátých letech minulého století. V té době se snažily definovat především východiska a pochopit celý rozsah problému [9]. Ukázalo se, že problém dlouhodobého uchování digitálních dokumentů je rozsáhlejší a komplexnější než se jevilo na počátku a zahrnuje v sobě řadu oborů, počínaje legislativou, státní správou, přes archivnictví a knihovnictví, až k informačním technologiím, které tvoří jádro řešení. Jako hlavní výzvy v této oblasti se ukázaly:

- Legislativní požadavky (založené na tradičním vnímání dokumentů) jsou často v rozporu s technickými možnostmi
- Vývoj v IT způsobuje ztrátu čitelnosti, případně i zabezpečení uložených dokumentů, je nutné sledovat vývoj a přizpůsobovat se mu, aby informace byly uchovány použitelné, ale přitom je také nutné zachovat jejich autentičnost
- Komplexnost architektury archivu, která musí zajistit řadu funkcí, jak v oblasti uložení dat, tak jejich správy a přístupu k nim, a svým rozsahem se vyrovná takový systém složitým podnikovým informačním systémům
- Organizační struktura, procesy a postupy archivu v oblasti digitálních dat jsou nezbytnou součástí funkčního celku, přitom ale nejsou dobře definovány a jejich rozsah je značný a přináší nové problémy neznámé v předchozích řešeních.

Po projektech vymezujících potřebný rámec digitální archivace následovaly projekty, které se soustředily na některé aspekty dlouhodobé archivace, ale prakticky neexistuje projekt který by vyřešil všechny aspekty v rámci jednoho integrovaného řešení.

Projekty v této oblasti buď vznikaly z potřeby organizací zodpovědných za uchovávání informací (knihovny, archivy aj.) [10],, které byly postaveny před aktuální potřebu uchovávat elektronické dokumenty, které vznikaly v oblasti jejich působnosti. Tyto projekty se často vyznačují určitou mírou pragmatičnosti, kdy se autoři snaží přijít s řešením, které by pokrylo jejich momentální potřeby s tím, že bude možný jeho vývoj do budoucna a rozšíření o další funkcionalitu.

Další kategorie projektů se zaměřuje na některý aspekt dlouhodobé archivace, ať již technický [13], nebo procesní [12].Tyto projekty jsou typicky součástí výzkumných programů a přinášejí nové technologie a postupy v této oblasti.

Dále také běží projekty, které se snaží vytvořit referenční softwarové prostředí [13], dostupné jako otevřený zdrojový kód, které může sloužit jako rámec pro implementaci digitálního archivu.

5. Technické a organizační podmínky dlouhodobého uchování elektronických dokumentů

Při posuzování vlivu vlastností informačního systému na důvěryhodnost digitálního archivu jako celku lze vycházet ze základního rozdělení vlastností na:

- Funkční vlastnosti - Jedná se o ty vlastnosti, které plní funkce z hlediska procesů archivu. Funkční požadavky vychází z politiky a postupů archivu, které zase vychází z životního cyklu digitálního dokumentu. Z hlediska funkčních vlastností je především důležité, aby tyto byly **ve shodě** s procesy archivu a aby poskytovaly **podporu** procesům archivu. Přestože tento požadavek se jeví jako samozřejmý, v praxi není často dodržen a řada procesů je naopak přizpůsobena vlastnostem dostupných systémů, a tak řada kroků v rámci procesu je pak buď nevyhovující nebo nadbytečná.
- Obecné (nefunkční) vlastnosti - Jsou obecné vlastnosti informačních systémů, společné většině implementací, které celkově ovlivňují chování systému.

Mezi hlavní nefunkční vlastnosti, důležité pro posuzování systému digitálního archivu, patří (seřazeny podle důležitosti):

- Vysoká spolehlivost a dostupnost
- Bezpečnost
- Škálovatelnost
- Účtovatelnost/Auditovalenost
- Snadná spravovatelnost

Výše jmenované obecné vlastnosti systému tvoří pouze rámcové východisko pro posuzování podmínek důvěryhodnosti v systému digitálního archivu, podrobnější specifikace jak vlastností informačního systému, tak navazujících procesů je specifikována v řadě mezinárodních standardů a doporučení, které lze využít pro detailnější specifikace systémů digitálního archivu. Relevantní dokumenty z této oblasti lze rozdělit do tří oblastí:

- Normy a doporučení týkající se dlouhodobé archivace nebo uchování elektronických dokumentů (sem patří například ISO/TR 15801 [14], ISO/TR 18492 [15] a RLG doporučení pro důvěryhodná digitální úložiště [1])
- Normy a doporučení týkající se systémů správy záznamů (Record Management), kdy archivní systémy mají v řadě aspektů blízko k těmto systémům (jedná se např. o Evropské doporučení Moreq [16] nebo ISO 18459 [17])
- Normy a doporučení týkající se bezpečnosti IS (jako je např. ISO/IEC 17799 [18])

Kromě obecných podmínek popsaných výše, které jsou známy i z řady jiných systémů, musí systém archivu používat řadu dalších specifických technologií a postupů, které jsou úzce zaměřeny na dlouhodobé uchování elektronických dokumentů:

- Uchování nezávislé využitelnosti formátu elektronického dokumentu
- Metadata
- Média pro uložení elektronických dokumentu
- Zabezpečení dat, metadat a komunikačních protokolů během životního cyklu elektronického dokumentu

Projekt se detailně zbýval těmito jednotlivými technologiemi a detailní informace lze získat ze závěrečné zprávy projektu [Projekt].
Projekt se také detailně zabýval organizací a organizační infrastrukturou archivu a procedurami, procesy a funkcí archivu, kdy opět lze detaily nalézt v závěrečné zprávě projektu [Projekt].

6. References

[Projekt] Dlouhodobé uchovávání elektronických dokumentů se zaručeným elektronickým podpisem, http://digiarchiv.eu/

[1] LRG : Research Libraries Group. (2002). Trusted digital repositories: Attributes and responsibilities. An RLG-OCLC Report. Available at: http://www.rlg.org/longterm/repositories.pdf

[2] DOMEA-Konzept (Requirement Catalogue 2.0, 2005), http://www.kbst.bund.de/cln_006/nn_836802/SharedDocs/Anlagen-kbst/Domea/domea-requirements-catalogue-2-0,templateId=raw,property=publicationFile.pdf/domea-requirements-catalogue-2-0.pdf

[3] www.uncitral.org/english/texts/electcom/ml-ecomm.htm

[4] Směrnice EU č. 2004/17/EC převzala definici písemnosti (Čl. I odst. 11)

[5] viz § 3, § 3a a § 4 zákona o elektronických komunikací

[6] viz Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce, Čl. 6

[7] viz např. R v Spiby (1990) 91 Cr.App. R186; nebo R v Shepherd (1993) 1 All ER 225

[8] viz např. L'archivage electronique, Frédéric Mascré, září 2003

[9] Např. projekty jako RLG – "Trusted digital repositories", OAIS a další

[10] Jako holandský DNEP a navazující evropský projekt NEDLIB, australská PANDORA, americký projekt NARA a řada dalších

[11] Např. uchování bezpečnosti – ArchiSig, OpenEvidence, metadata – METS, PREMIS atd.

[12] Např. INTERPARES, DOMEA

[13] Jako je např. FEDORA nebo DSpace

[14] ISO/TR 15801:2004 Electronic imaging -- Information stored electronically -- Recommendations for trustworthiness and reliability

[15] ISO/TR 18492:2005 Long-term preservation of electronic document-based information

[16] MoReq SPECIFICATION - MODEL REQUIREMENTS FOR THE MANAGEMENT OF ELECTRONIC RECORDS, IDA Programme, CECA-CEE-CEEA, Bruxelles-Luxembourg, 2001

[17] ISO 15489-1:2001Information and documentation -- Records management -- Part 1: General, ISO/TR 15489-2:2001Information and documentation -- Records management -- Part 2: Guidelines

[18] ISO/IEC 17799, Information technology-Security techniques-Code of Practice

C. Rozhovor na téma bezpečnost našich webmailů

V lednu 2008 jste mohli zaznamenat zprávy o bezpečnostních testech, které proběhly na českých a slovenských webmailech (viz např. vysílání TV NOVA 18.1.2008 http://www.nova.cz/tvarchiv/?238d=18.01.2008&238m=p&238p=ODPOLEDNITN&238v=126862). Tyto testy provedl administrátor informačního portálu SOOM.cz, který vystupuje pod pseudonymem .cCuMiNn. Ten také jejich výsledek uveřejnil na stránkách portálu SOOM.cz (http://www.soom.cz/index.php?name=articles/show&aid=472) a dal tak uživatelům možnost zjistit, jak si na tom s bezpečností aktuálně stojí konkrétní poskytovatelé webmailu. Všeobecně by se dalo říci, že zmiňovaný report bezpečnost v testovaných webmailech silně kritizuje. Podle autora dokáže v současné době napadnout soukromí uživatelů v tuzemských webmailech každý i méně zkušený cracker.

Položili jsme proto autorovi testů a zveřejněného reportu pár dotazů, abychom se dozvěděli některé podrobnosti ohledně celé této kauzy.

Co Vás k provedení bezpečnostních testů přimělo?

Celá záležitost začala již před více než půl rokem, kdy jsem testoval nově nabyté vědomosti ve webmailu společnosti Seznam.cz. Tehdy se mi v jejich aplikaci podařilo nalézt zranitelnost v podobě CSRF, na kterou jsem prostřednictvím portálu SOOM.cz upozornil. Komunikace s provozovatelem webmailu Seznam.cz probíhala na úrovni a z celé záležitosti jsem si odnesl příjemný pocit. O pár měsíců později jsem se zaměřil na bezpečnost webu Volny.cz, který mě omrácil neuvěřitelným počtem zranitelností v podobě XSS, jež byly roztroušeny po celém webu. Po předchozí zkušenosti z komunikace se společností Seznam.cz jsem tentokrát upozornil na nalezené chyby skrz hotline pár dní před tím, než jsem výsledek testu zveřejnil na webu. Ze strany Volny.cz jsem ale neobdržel žádnou odpověď a dokonce i ohlášené chyby začaly být opravovány teprve ve chvíli, kdy došlo k jejich zveřejnění. Následovalo vytvoření exploitu, který ve webmailu Volny.cz zneužíval téměř rok starou zranitelnost, o níž provozovatel Volny.cz věděl, ale přesto nepodniknul kroky vedoucí k jejímu odstranění. Opět se celou věcí začali zabývat teprve ve chvíli, kdy byl exploit volně k dispozici. činnost vývojářů mi ovšem při odstraňování zranitelnosti připadala jako vyrážení klínu klínem a zdálo se, že vývojáři nejsou schopni chybu úspěšně zapatchovat. I po jejich zákroku, bylo stále s menšími úpravami možné exploit použít. To mě přivedlo na myšlenku, že to s úrovní bezpečnosti v našich webmailech nemusí být tak růžové, jak by si většina uživatelů představovala a vrhnul jsem se proto do testů, které měly obsáhnout většinu našich větších poskytovatelů.

Jakým způsobem jste testy prováděl?

Připravil jsem si asi 20 e-mailových zpráv, které obsahovaly skripty v různých částech mailu. Konkrétně to bylo v hlavičkách FROM, TO a SUBJECT, pak také například v názvu přiloženého souboru nebo v těle zprávy. Tyto maily jsem odeslal do schránek, které jsem si pro tento účel na freemailech vytvořil a následně jsem zevrubně otestoval různá vstupní pole ve webovém rozhraní, zda neobsahují náchylnost na útoky XSS a zranitelnosti typu CSRF. Oba tyto útoky mohou v případě úspěchu vyvolat změny v uživatelském nastavení účtu a já byl překvapen, kolik z těchto jednoduchých útoků uspělo. Někdo by mohl namítat, že pokud testy nebyly provedeny kompletně, není možné jednotlivé webmaily srovnávat. Je však potřeba si uvědomit, že nad kompletními testy bych u tolika webmailů strávil možná i rok, což nebylo možné. Domnívám se, že provedený test dokázal dostatečně vylíčit stav

zabezpečení a je už jen na jednotlivých poskytovatelích, aby dohledali další slabiny ve svých aplikacích.

Na jaké úrovni je podle Vás zabezpečení našich webmailů?
Odpověď na tuto otázku vyplývá ze samotného reportu. Bezpečnost našich webmailů je dle mého naprosto mizerná. Když si uvědomíme, že ze zaslaných dvaceti e-mailových zpráv se v průměru třem až čtyřem z nich podařilo spustit úspěšný útok, není ani možné si o jejich zabezpečení myslet nic jiného. Ke všemu nešlo z mé strany o hlubší průzkum aplikací webmailů, ale skutečně jen o rychlý test zranitelností, kterých by byl schopen každý, kdo má alespoň základní představu o struktuře e-mailové zprávy a ovládá javascript na úrovni začátečníka. Některé z nalezených zranitelností jsou přesto natolik závažné, že útočníkovi umožňují plné ovládnutí uživatelského účtu bez jakékoliv spoluúčasti napadeného.

Jaká byla ze strany poskytovatelů odezva?
Jednotlivé reakce by se dali rozdělit do třech skupin. Někteří z poskytovatelů se ozvali, aby zjistili, kde se nachází slabá místa v jejich aplikaci. Jiní napadali objektivnost testu a měli k němu mnoho připomínek. No a konečně třetí a asi největší skupina se skládala z těch, kteří na provedené testy nereagovali vůbec. Zajímalo by mě, zda se tito o testech nedozvěděli, nebo zda prostě nemají snahu se zabezpečením svých aplikací něco udělat.

Která z reakcí Vám udělala největší radost?
Takových reakcí bylo hned několik, ale asi největší dojem na mě udělal poskytovatel webmailu Atlas.cz a to hned z několika důvodů. Z hlediska zařazení by sice patřil nejvíce do druhé skupiny. To je mezi ty, kteří se snažili mnou provedené testy zpochybnit, o čemž mluví i tisková zpráva, která byla zveřejněna na webu Atlas.cz. Ta nejenom, že zpochybňuje výsledky testů a jejich objektivnost, ale snaží se zpochybnit i existenci samotných zranitelností. Na druhou stranu ovšem bylo z reakcí Atlasu patrné, že jde této společnosti o bezpečnost v první řadě. Byl zájem o oznámení mnou nalezených zranitelností a došlo ze strany společnosti i k dalšímu vyhledávání míst, která by mohla být zneužita. Veškeré chyby byly téměř okamžitě z tohoto webmailu odstraněny a tak by si dnes určitě zasloužil lepší hodnocení, než jakého se mu dostalo. Největší radost mi tedy udělaly ty společnosti, které zranitelnosti ze svých aplikací odstranili a pro uživatele tak vytvořily bezpečnější místo, kde se nebudou muset bát ukládat své soukromé e-maily.

Jaké máte plány do budoucna?
Zcela jistě projdu bezpečnost na testovaných webmailech ještě jednou, abych zjistil, jaká opatření byla provozovateli provedena. Na základě zjištěných informací zveřejním nový report, který by měl podávat nové srovnání bezpečnosti po šanci na sjednání nápravy, kterou poskytovatelé dostali. Po té již nebude pochyb o tom, kde je bezpečné místo pro e-maily uživatelů a kde bohužel ne. Vzhledem k tomu, že jsem obdržel i řadu žádostí o otestování bezpečnosti webmailů, které v mém testu nebyly zastoupeny, začal jsem také pracovat na projektu, s jehož pomocí si bude moci otestovat výskyt některých zranitelností ve webmailu kterýkoliv uživatel. Věřím, že tato aplikace povede opět ke zvýšení bezpečnosti na Internetu.

Otázky autorovi testů kladl: Pavel Vondruška (pavel.vondruska@crypto-world.info)

D. O čem jsme psali v únoru 2000 – 2007

Crypto-World 2/2000

A.	Dokumenty ve formátu PDF (M.Kaláb)	2
B.	Kevin Mitnick na svobodě (P.Vondruška)	3
C.	Velká Fermatova věta (historické poznámky) (P.Vondruška)	4
D.	Fermat Last Theorem (V.Sorokin)	5
E.	Zákon o elektronickém podpisu otevírá cestu do Evropy ? (Souček, Hrubý, Beneš, Vondruška)	6-8
F.	Letem šifrovým světem	9-10
G.	Závěrečné informace	11

Crypto-World 2/2001

A.	CRYPTREC - japonská obdoba NESSIE (informace) (J.Pinkava)	2 - 3
B.	Připravované normy k EP v rámci Evropské Unie II. (J.Pinkava)	4 - 6
C.	K návrhu zákona o elektronickém podpisu, jeho dopadu na ekonomiku a bezpečnostních hlediscích (J.Hrubý, I.Mokoš)	7 - 14
D.	Mobilní telefony (komunikace, bezpečnost) (J.Kobelka)	15- 17
E.	NIST software pro statistické testování náhodných a pseudonáhodných generátorů pro kryptografické účely (J.Pinkava)	18 - 27
F.	Letem šifrovým světem	27 - 28
G.	Závěrečné informace	29

Crypto-World 2/2002

A.	Vyhláška č.366/2001 Sb., bezpečný prostředek pro vytváření elektronického podpisu a nástroj elektronického podpisu (P.Vondruška)	2 - 8
B.	RUNS testy (P.Tesař)	9 -13
C.	Velikonoční kryptologie (V.Matyáš)	13
D.	Terminologie (V.Klíma)	14
E.	Letem šifrovým světem	15-16
F.	Závěrečné informace	17

Příloha: Program pro naše čtenáře : "Hašák ver. 0.9" (viz. letem šifrovým světem) hasak.

Crypto-World 2/2003

A.	České technické normy a svět, II.část (Národní normalizační proces) (P.Vondruška)	2 - 4
B.	Kryptografie a normy. Digitální certifikáty. IETF-PKIX část 9. Protokol SCVP (J.Pinkava)	5 -10
C.	Faktorizace a zařízení TWIRL (J.Pinkava)	11-12
D.	NIST - dokument Key Management	13-16
E.	Letem šifrovým světem	17-21

- Kurs "kryptologie" na MFF UK Praha
- Za použití šifrování do vězení
- Hoax jdbgmgr.exe
- Interview
- AEC uvedla do provozu certifikační autoritu TrustPort

- 6. ročník konference - Information Systems Implementation and Modelling ISIM'03
- O čem jsme psali v únoru 2000 - 2002
F. Závěrečné informace 22
Příloha : Crypto_p2.pdf
Přehled dokumentů ETSI, které se zabývají elektronickým podpisem
(ETSI - European Telecommunication Standards Institute) 10 stran

Crypto-World 2/2004

A. Opožděný úvodník (P.Vondruška) 2-4
B. Jak jsem pochopil ochranu informace (T.Beneš) 5-9
C. Požadavky na politiku poskytovatele, který vydává atributové certifikáty, které lze používat spolu s kvalifikovanými certifikáty (Technical report ETSI 102 158), Část 2. (J.Pinkava) 10-13
D. Archivace elektronických dokumentů, část 3. (J.Pinkava) 14-15
E. IFIP a bezpečnost IS (D.Brechlerová) 16-17
F. Letem šifrovým světem 18-22
- Novinky (23.1.2004-14.2.2004)
- O čem jsme psali v únoru 2000 - 2003
G. Závěrečné informace 23

Crypto-World 2/2005

A. Mikulášská kryptobesídka 2004 (V. Matyáš, D. Cvrček) 2-3
B. Útoky na šifru Hiji-bij-bij (HBB) (V. Klíma) 4-13
C. A Concise Introduction to Random Number Generators (P. Hellekalek) 14-19
D. Útoky na a přes API: PIN Recovery Attacks (J. Krhovják, D. Cvrček) 20-29
E. MoraviaCrypt'05 (CFP) 30
F. O čem jsme psali v únoru 2000-2004 31
G. Závěrečné informace 32

Crypto-World 2/2006

A. Statistika vydaných elektronických podpisů (P.Vondruška) 2-5
B. Kryptologie, šifrování a tajná písma (P.Vondruška) 6-8
C. NIST (National Institute of Standards and Technology - USA) a kryptografie, část 1. (J.Pinkava) 9-12
D. E-Mudžahedínové, virtuální strana štěstí a e-sprejeři … (P.Vondruška) 13-16
E. O čem jsme psali v únoru 1999-2005 17
F. Závěrečné informace 18

Crypto-World 2/2007

A. Najväčšia tma je pod lampou – STEGANOGRAFIA, část I. (R.Cinkais) 2-9
B. XML bezpečnost, část II. (D. Brechlerová) 10-20
C. Přehled dokumentů ETSI v oblasti elektronického podpisu, časových razítek a kvalifikovaných certifikátů (V.Sudzina) 21-22
D. O čem jsme psali v únoru 2000 - 2006 23-24
E. Závěrečné informace 25

E. Závěrečné informace

1. Sešit

Crypto-World je oficiální informační sešit "Kryptologické sekce Jednoty českých matematiků a fyziků" (GCUCMP). Obsahuje články podepsané autory. Případné chyby a nepřesnosti jsou dílem P.Vondrušky a autorů jednotlivých podepsaných článků, GCUCMP za ně nemá odbornou ani jinou zodpovědnost.
Adresa URL, na níž můžete najít tento sešit (zpravidla 3 týdny po jeho rozeslání) a předchozí sešity GCUCMP, denně aktualizované novinky z kryptologie a informační bezpečnosti, normy, standardy, stránky některých členů a další související materiály:
http://crypto-world.info

2. Registrace / zrušení registrace

Zájemci o e-zin se mohou zaregistrovat pomocí e-mailu na adrese pavel.vondruska@crypto-world.info (předmět: Crypto-World) nebo použít k odeslání žádosti o registraci elektronický formulář na http://crypto-world.info. Při registraci vyžadujeme pouze jméno a příjmení, titul, pracoviště (není podmínkou) a e-mail adresu určenou k zasílání kódů ke stažení sešitu.
Ke zrušení registrace stačí zaslat krátkou zprávu na e-mail pavel.vondruska@crypto-world.info (předmět: ruším odběr Crypto-Worldu!) nebo opět použít formulář na http://crypto-world.info. Ve zprávě prosím uveďte jméno a příjmení a e-mail adresu, na kterou byly kódy zasílány.

3. Redakce

E-zin Crypto-World

Redakční práce:	Pavel Vondruška
Stálí přispěvatelé:	Pavel Vondruška
	Jaroslav Pinkava
Jazyková úprava:	Jakub Vrána
Přehled autorů:	http://crypto-world.info/obsah/autori.pdf
NEWS	Vlastimil Klíma
(výběr příspěvků,	Jaroslav Pinkava
komentáře a	Tomáš Rosa
vkládání na web)	Pavel Vondruška
Webmaster	Pavel Vondruška, jr.

4. Spojení (abecedně)

redakce e-zinu	ezin@crypto-world.info ,	http://crypto-world.info
Vlastimil Klíma	v.klima@volny.cz ,	http://cryptography.hyperlink.cz/
Jaroslav Pinkava	Jaroslav.Pinkava@zoner.cz ,	http://crypto-world.info/pinkava/
Tomáš Rosa	t_rosa@volny.cz ,	http://crypto.hyperlink.cz/
Pavel Vondruška	pavel.vondruska@crypto-world.info ,	http://crypto-world.info/vondruska/index.php
Pavel Vondruška,jr.	pavel@crypto-world.info ,	http://webdesign.crypto-world.info
Jakub Vrána	jakub@vrana.cz ,	http://www.vrana.cz/